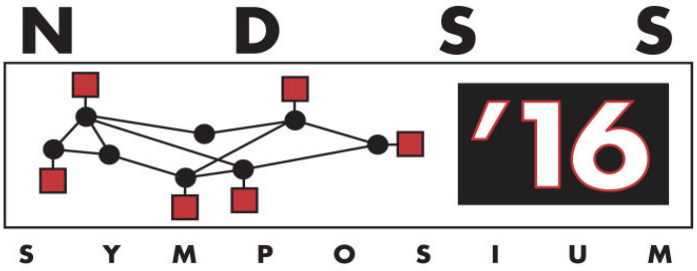
Proceedings

2016

Network and Distributed System Security Symposium



Proceedings

2016

Network and Distributed System Security Symposium

February 21 – 24, 2016

San Diego, California

Sponsored by the
Internet Society

Internet Society
1775 Wiehle Avenue
Suite 201
Reston, VA 20190-5108

Address your correspondence to: Senior Events Manager, Internet Society, 1775 Wiehle Avenue, Suite 201, Reston, Virginia 20190-5108, U.S.A., tel. +1 703 439 2120, fax +1 703 326 9881, ndss@isoc.org.

The papers included here comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interest of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors or the Internet Society.

ISBN Number (Digital Format) : 1-891562-41-X

Additional copies may be ordered from:

Internet Society
1775 Wiehle Avenue
Suite 201
Reston, VA 20190-5108
tel +1 703.439.2120
fax +1 703.326.9881
http://www.internetsociety.org

Proceedings of the 2016 Network and Distributed System Security Symposium

Table of Contents

It's Free for a Reason: Exploring the Ecosystem of Free Live Streaming Services
M.Z. Rafique, T. Van Goethem, W. Joosen, C. Huygens, N. Nikiforakis

Attack Patterns for Back-Box Security Testing of Multi-Party Web Applications
A. Sudhodanan, A. Armando, R. Carbone, L. Compagna

Are these Ads Safe: Detecting Hidden Attacks through the Mobile App-Web Interfaces
V. Rastogi, R. Shao, Y. Chen, X. Pan, S. Zou, R. Riley

SESSION 4: Network Security Part II

Enabling Practical Software-defined Networking Security Applications with OFX
J. Sonchack, A.J. Aviv, E. Keller, J.M. Smith

Forwarding-Loop Attacks in Content Delivery Networks
J. Chen, J. Jiang, X. Zheng, H. Duan, J. Liang, K. Li, T. Wan, V. Paxson

CDN-on-Demand: An affordable DDoS Defense via Untrusted Clouds
Y. Gilad, A. Herzberg, M. Sudkovitch, M. Goberman

Towards SDN-Defined Programmable BYOD (Bring Your Own Device) Security
S. Hong, R. Baykov, L. Xu, S. Nadimpalli, G. Gu

SESSION 5: MISC: Cryptocurrencies, Captchas, and GameBots

Centrally Banked Cryptocurrencies
G. Danezis, S. Meiklejohn

Equihash: Asymmetric Proof-of-Work Based on a Generalized Birthday Problem
A. Biryukov, D. Khovratovich

A Simple Generic Attack on Text Captchas
H. Gao, J. Yan, F. Cao, Z. Zhang, L. Lei, M. Tang, P. Zhang, X. Zhou, X. Wang, J. Li

You are a Game Bot! Uncovering Game Bots in MMORPGs via Self-similarity in the Wild
E. Lee, J. Woo, H. Kim, A. Mohaisen, H.K. Kim

SESSION 6: Privacy in Mobile

Tracking Mobile Web Users Through Motion Sensors: Attacks and Defenses
A.Das, N. Borisov, M. Caesar

The Price of Free: Privacy Leakage in Personalized Mobile In-Apps Ads
W. Meng, R. Ding, S.P. Chung, S. Han, W. Lee

What Mobile Ads Know About Mobile Users
S. Son, D. Kim, V. Shmatikov

Free for All! Assessing User Data Exposure to Advertising Libraries on Android
S. Demetriou, W. Merrill, W. Yang, A. Zhang, C.A. Gunter

Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems
A.Shaik, R. Borgaonkar, N. Asokan, V. Niemi, J-P. Seifert

SESSION 7: Software Security

Towards Automated Dynamic Analysis for Linus-based Embedded Firmware
D.D. Chen, M. Egele, M. Woo, D. Brumley

discovRE: Efficient Cross-Architecture Identification of Bugs in Binary Code
S. Eschweiler, K. Yakdan, E. Gerhards-Padilla

Driller: Augmenting Fuzzing Through Selective Symbolic Execution
N. Stephens, J. Grosen, C. Salls, A. Dutcher, R. Wang, J. Corbetta, Y. Shoshitaisvili, C. Kruegel, G. Vigna

VTrust: Regaining Trust on Virtual Calls
C. *Zhang, S.A. Carr, T. Li, Y. Ding, C. Song, M. Payer, D. Song*

Protecting C++ Dynamic Dispatch Through VTable Interleaving
D. Bounov, R. Gökhan Kici, S. Lerner

SESSION 8: System Security – Part I

ProTracer: Towards Practical Provenance Tracing by Alternating Between Logging and Tainting
S. Ma, X. Zhang, D. Xu

Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems
D. Formby, P. Srinivasan, A. Leonard, J. Rogers, R. Beyah

SKEE: A Lightweight Secure Kernel-level Execution Environment for ARM
A. Azab, K. Swidowski, R. Bhutkar, J. Ma, W. Shen, R. Wang, P. Ning

OpenSGX: An Open Platform for SGX Research
P. Jain, S. Desai, S. Kim, M-W. Shih, JH. Lee, C. Choi, Y. Shin, T. Kim, B.B. Kang, D. Han

SESSION 9: Privacy – Part I

Efficient Private Statistics with Succinct Sketches
L. Melis, G. Danezis, E. De Cristofaro

Dependence Makes You Vulnerable: Differential Privacy Under Dependent Tuples
C. Liu, S. Chakraborty, P. Mittal

Privacy-Preserving Shortest Path Computation
D.J. Wu, J. Zimmerman, J. Planul, J.C. Mitchell

LinkMirage: Enabling Privacy-preserving Analytics on Social Relationships
C.Liu, P. Mittal

SESSION 10: Privacy – Part II

Do You See What I See? Differential Treatment of Anonymous Users
S. Khattak, D. Fifield, S. Afroz, M. Javed, S. Sundaresan, V. Paxson, S.J. Murdoch, D. McCoy,

Measuring and Mitigating AS-level Adversaries Against Tor
R. Nithyanand, O. Starov, A. Zair, P. Gill, M. Schapira

Website Fingerprinting at Internet Scale
A. Panchenko, F. Lanze, A. Zinnen, M. Henze, J. Pennekamp, K. Wehrle, T. Engel

SESSION 11: Malware

Extract Me If You Can: Abusing PDF Parsers in Malware Detectors
C. Carmony, M. Zhang, X. Hu, A.V. Bhaskar, H.Yin

Automatically Evading Classifiers: A Case Study on PDF Malware Classifiers
W. Xu, Y. Qi, D. Evans

Cache, Trigger, Impersonate: Enabling Context-Sensitive Honeyclient Analysis On-the-Wire
T. Taylor, K.Z. Snow, N. Otterness, F. Monrose

LO-PHI: Low-Observable Physical Host Instrumentation for Malware Analysis
C. Spensky, H. Hu, K. Leach

When a Tree Falls: Using Diversity in Ensemble Classifiers to Identify Evasion in Malware Detectors
C. Smutz, A. Stavrou

SESSION 12: System Security – Part II

Kratos: Discovering Inconsistent Security Policy Enforcement in the Android Framework
Y. Shao, J. Ott, Q.A. Chen, Z. Qian, Z.M. Mao

How to Make ASLR Win the Clone Wars: Runtime Re-Randomization
K. Lu, S. Nürnberger, M. Backes, W. Lee,

Leakage-Resilient Layout Randomization for Mobile Devices
K. Braden, S. Crane, L. Davi, M. Franz, P. Larsen, C. Liebchen, A-R. Sadeghi

Enabling Client-Side Crash-Resistance to Overcome Diversification and Information Hiding
R. Gawlik, B. Kollenda, P. Koppe, B. Garmany, T. Holz

Enforcing Kernel Security Invariants with Data Flow Integrity
C. Song, B.Lee, K. Lu, W. Harris, T. Kim, W. Lee

SESSION 13: Android Security

Going Native: Using a Large-Scale Analysis of Android Apps to Create a Practical Native-Code Sandboxing Policy
V. Afonso, A. Bianchi, Y. Fratantonio, A. Doupe, M. Polino, P. de Geus, C. Kruegel, G. Vigna

Life after App Uninstallation: Are the Data Still Alive? Data Residue Attacks on Android
X. Zhang, K. Ying, Y. Aafer, Z. Qiu, W. Du

FLEXDROID: Enforcing In-App Privilege Separation in Android
J. Seo, D. Kim, D. Cho, T. Kim, I. Shin

IntelliDroid: A Targeted Input Generator for the Dynamic Analysis of Android Malware
M.Y. Wong, D. Lie

Harvesting Runtime Values in Android Applications That Feature Anti-Analysis Techniques
S. Rasthofer, S. Arzt, M. Miltenberger, E. Bodden

SESSION 14: User Authentication

Automatic Forgery of Cryptographically Consistent Messages to Identify Security Vulnerabilities in Mobile Services
C. Zuo, W. Wang, R. Wang, Z. Lin

Differentially Private Password Frequency Lists
J. Blocki, A. Datta, J. Bonneau

Who Are You? A Statistical Approach to Measuring User Authenticity
D. Freeman, S. Jain, M. Duermuth, B. Biggio, G. Giacinto

Pitfalls in Designing Zero-Effort Deauthentication: Opportunistic Human Observation Attacks
O. Huhta, P. Shrestha, S. Udar, M. Juuti, N. Saxena, N. Asokan

VISIBLE: Video-Assisted Keystroke Inference from Tablet Backside Motion
J. Sun, X. Jin, Y. Chen, J. Zhang, R. Zhang, Y. Zhang

General Chair's Message

It is my pleasure to welcome you to the 23rd Annual Network and Distributed System Security Symposium.

I'm happy to report that this year's NDSS has the most content to offer of any NDSS meeting so far. Building on the success of previous years, this year we have three collocated workshops: TLS 1.3 Ready or Not (TRON), Understanding and Enhancing Online Privacy (UEOP), and Usable Security (USEC). The workshops span a broad range, some focused on traditional academic research, others focused on the concerns of practitioners; some publishing proceedings, others more informal and interactive. I'd like to thank Matthew Smith, the Workshop Chair, for bringing together such an exciting set of workshops.

Also building on recent success, we're this year continuing the tradition of organizing a poster session to showcase both in-progress and exciting recent work in various aspects of computer security. Thanks are due to Manuel Egele and Michelle Mazurek, the Poster Co-Chairs, for making sure we have an excellent poster program.

Due to increased interest in our field and in NDSS, more papers will be presented at NDSS this year than in any past year, yielding a particularly rich and exciting program. Selecting the papers is a task that involves many people and many hours of hard work. I'd like to thank Srdjan Capkun, the Program Chair, for the tremendous amount of work he donated and the excellent job he's done in putting together this year's program.

Many individuals have contributed to making NDSS a success, including everyone on the Steering Group, Organizing Committee, and many Internet Society staff; all have my gratitude. I'd like to specifically thank a few with whom I've worked closely and whose contributions have been particularly noteworthy: Karen O'Donoghue and David Balenson. Karen O'Donoghue has put in a tremendous amount of work and dealt with an ever-growing number of minor crises and unforeseen challenges in coordinating the Internet Society's role in organizing the conference. David Balenson has regularly exceeded what was expected of him, stepping in to help with tasks that weren't even vaguely related to his role as Publications Chair.

NDSS is possible in large part thanks to our generous sponsors. I'd like to thank Cisco, Afilias, Check Point Software Technologies, San Diego Supercomputer Center, Qualcomm and Mozilla for their ongoing support, and the Internet Society for hosting the symposium. Funds for our student grants were provided by the National Science Foundation and the Internet Society.

Finally, thank you, all, for participating in the symposium and through that adding the key ingredient that makes NDSS a success. I wish you all an excellent 23rd NDSS!

.

Lujo Bauer
General Chair, NDSS'16
Carnegie Mellon University

Program Chair's Message

It gives me great pleasure to welcome you to the 23nd Annual Network & Distributed System Security Symposium (NDSS 2016). This year's edition of NDSS is held at the Catamaran Resort Hotel and Spa in San Diego, CA, United States on February 21-24, 2016. NDSS fosters information exchange among researchers and practitioners of network and distributed system security. The target audience includes those interested in practical aspects of network and distributed system security, with a focus on actual system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of network and distributed systems security technologies.

NDSS is one of the prime security venues and I was honored to chair this year's program committee. The committee consisted of 43 researchers with established track records in a broad range of security and related topics. This year, NDSS received 389 submissions which were evaluated on the basis of their technical quality, novelty, and significance. Papers were evaluated in several rounds. In order to allow authors time to improve their work and submit to other venues, authors of submissions for which there is a consensus on rejection were notified after the first round of reviews and discussions. The paper selection process was finalized during a one-and-a-half-day in-person program committee meeting in New York, at which 60 papers (approximately 15.5%) were selected to appear at NDSS 2016.

Selecting a high-quality conference program is inherently a community effort and I am grateful to all those who supported this effort or actively took part in the selection process: Ari Juels for shadow-chairing the event, for his effort, support and patience - thanks Ari! Two Sigma for hosting the PC meeting in their amazing premises. Nikos Karapanos and Claudio Marforio for setting up the reviewing infrastructure, and for their assistance through the whole process. Lujo Bauer for his advice and guidance. Terry Weigler and Karen O'Donoghue for their logistical support. David Balenson, NDSS Publications Chair for his effort with the proceedings. I would further like to thank the program committee members for their great work. It has been a true pleasure to work in such a committee. Finally, great thanks to the authors who submitted their work to NDSS, the attendees and the readers of these proceedings!

Srdjan Capkun
Program Chair, NDSS'16
ETH Zurich

Program Committee

Srdjan Capkun, *ETH Zurich* (Program Chair)
Ari Juels*, Cornell Tech* (Shadow Chair)

Manos Antonakakis, *Georgia Institute of Technology*

Davide Balzarotti, *EURECOM*

Lujo Bauer, *Carnegie Mellon University*

Joseph Bonneau, *Stanford University and EFF*

Nikita Borisov, *University of Illinois at Urbana-Champaign*

Kevin Butler, *University of Florida*

Nicolas Christin, *Carnegie Mellon University*

Emiliano De Cristofaro, *University College London*

William Enck, *North Carolina State University*

Manuel Egele, *Boston University*

Guofei Gu, *Texas A&M University*

Thorsten Holz, *Ruhr-University Bochum*

Somesh Jha, *University of Wisconsin Madison*

Jonathan Katz, *University of Maryland*

Yongdae Kim, *KAIST*

Engin Kirda, *Northeastern University*

Farinaz Koushanfar, *Rice University*

Christopher Kruegel, *University of California, Santa Barbara*

Wenke Lee, *Georgia Institute of Technology*

Zhenkai Liang, *National University of Singapore*

David Lie, *University of Toronto*

Ben Livshits, *Microsoft Research*

Ivan Martinovic, *Oxford University*

Prateek Mittal, *Princeton University*

David Molnar, *Microsoft Research*

Cristina Nita-Rotaru, *Purdue University*

Alina Oprea, *RSA Laboratories*

Adrian Perrig, *ETH Zurich*

Christina Poepper, *Ruhr University Bochum*

Mike Reiter, *UNC Chapel Hill*

Thomas Ristenpart, *Cornell Tech*

Franziska Roesner, *University of Washington*

Andrei Sabelfeld, *Chalmers University*

Ahmad-Reza Sadeghi, *TU Darmstadt*

Reza Shokri, *University of Texas at Austin*

Robin Sommer, *International Computer Science Institute, Berkeley*

Patrick Traynor, *University of Florida*

Venkat Venkatakrishnan, *University of Illinois, Chicago*

Giovanni Vigna, *UC Santa Barbara*

David Wagner, *University of California, Berkeley*

XiaoFeng Wang, *Indiana University Bloomington*

Organizing Committee

General Chair

Lujo Bauer
Carnegie Mellon University

Program Chair

Srdjan Capkun
ETH Zurich

Workshop Chair

Matthew Smith
Rheinische Friedrich-Wilhelms-Universität Bonn

Poster Co-Chairs

Manuel Egele
Boston University

Michelle Mazurek
University of Maryland at College Park

Publications Chair and Historian

David Balenson
SRI International

Local Arrangements Chair

Thomas Hutton
San Diego Supercomputer Center
University of California, San Diego

Event Manager, Publicity Chair, and Sponsorship Coordinator

Karen O'Donoghue
Internet Society

Conference Coordinator

Terry Weigler
Internet Society

Steering Group

Co-Chairs

Lujo Bauer
Carnegie Mellon University

Karen O'Donoghue
Internet Society

Administrative Coordinator

Terry Weigler
Internet Society

Steering Group Members

Michael Bailey
University of Illinois Urbana-Champaign

David Balenson
SRI International

Davide Balzarotti
EURECOM

Srdjan Capkun
ETH Zurich

Deb Frincke
National Security Agency

Tom Hutton
San Diego Supercomputer Center

Yongdae Kim
Korea Advanced Institute of Science and Technology

Deborah Shands
Aerospace Corporation

Matthew Smith
University of Bonn

Paul Syverson
Naval Research Lab

Doug Szajda
University of Richmond

Helen Wang
Microsoft Research